

(19) 日本国特許庁 (J P)

## (12) 公開特許公報 (A)

(11) 特許出願公開番号  
特開2003-248578  
(P2003-248578A)

(43) 公開日 平成15年9月5日 (2003.9.5)

(51) Int Cl. <sup>7</sup>	識別記号	F I	テーマコード(参考)
G 0 6 F 7/58		G 0 6 F 7/58	A 5 B 0 3 5
G 0 6 K 19/10		G 0 9 C 1/00	6 5 0 B 5 J 1 0 4
G 0 9 C 1/00	6 5 0	G 0 6 K 19/00	R

審査請求 未請求 請求項の数10 O L 外国語出願 (全 18 頁)

(21) 出願番号 特願2002-347277(P2002-347277)  
 (22) 出願日 平成14年11月29日 (2002.11.29)  
 (31) 優先権主張番号 0 1 1 5 5 2 9  
 (32) 優先日 平成13年11月30日 (2001.11.30)  
 (33) 優先権主張国 フランス (F R)

(71) 出願人 591035139  
 エステーマイクロエレクトロニクス ソシエ  
 テ アノニム  
 フランス国, 92120 モンルーージュ, プー  
 ルパール ロマン ロラン, 29番地  
 (72) 発明者 リュク ヴィダール  
 フランス国, 83910 プウリール, ロ  
 ティスマン ル カド, 12番地  
 (74) 代理人 100074930  
 弁理士 山本 恵一

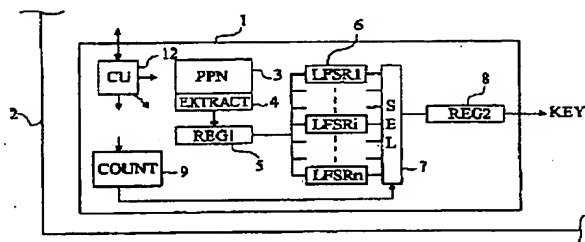
最終頁に続く

(54) 【発明の名称】 集積回路識別の秘密量の発生

## (57) 【要約】

【課題】 集積回路の識別子に基づいて秘密量を発生させる方法と回路を提供する。

【解決手段】 最初のデジタルワードは、物理パラメータネットワークから発生され、前記最初のワードは、少なくとも1つのシフトレジスタに提供され、前記シフトレジスタの出力が、秘密量を発生させる。



## 【特許請求の範囲】

【請求項 1】 集積回路 (2) の識別子に基づいて秘密量 (KEY) を発生する方法において、物理パラメータネットワーク (3) から最初のデジタルワードを発生させるステップと、前記最初のワードを少なくとも 1 つの逡及シフトレジスタ (6) に提示するステップとを含み、前記シフトレジスタの出力が前記秘密量を形成することを特徴とする方法。

【請求項 2】 前記最初のワードを複数の逡及シフトレジスタ (6) に提示し、それらシフトレジスタのうち 1 つを選択して前記秘密量 (KEY) を形成することを特徴とする請求項 1 に記載の方法。

【請求項 3】 前記選択は、先行の秘密量の破棄の後に変更されることを特徴とする、請求項 2 に記載の方法。

【請求項 4】 前記シフトレジスタ (6) は、線形逡及シフトレジスタであることを特徴とする請求項 1 に記載の方法。

【請求項 5】 セレクタ (7) によって複数のシフトレジスタのうち 1 つを選択することを特徴とする請求項 1 に記載の方法。

【請求項 6】 集積回路 (2) の内部で秘密量 (KEY) を発生する回路において、物理パラメータネットワーク (3) に基づく、集積回路チップに特定な最初のデジタルワードの発生器 (4) と、前記最初のワードを入力として受け取り、前記量を提供する少なくとも 1 つの逡及シフトレジスタ (6) と、カウンタ (9) によってプログラム可能で前記シフトレジスタのドリフトシーケンスのセレクタとを含むことを特徴とする回路。

【請求項 7】 集積回路 (2) の内部で秘密量 (KEY) を発生する回路において、物理パラメータネットワーク (3) に基づく、集積回路チップに特定な最初のデジタルワードの発生器と、前記最初の 2 進ワードを入力として受け入れる逡及シフトレジスタ (6) と、前記秘密量を提供する前記シフトレジスタのうちの 1 つを選択するセレクタ (7) とを含むことを特徴とする回路。

【請求項 8】 前記セレクタにより行われた選択は、秘密データが破棄された場合に変更されることを特徴とする請求項 6 に記載の回路。

【請求項 9】 セレクタ (7) は、前記シフトレジスタ (6) の入力／出力から、入力又は出力を選択するマルチプレクサにより形成されることを特徴とする請求項 7 に記載の回路。

【請求項 10】 請求項 6 に記載の回路において、前記最初のワード及び前記秘密量を記憶するレジスタ (5、8) は一時レジスタであり、

前記回路は、予め決められた時間の後で、それら一時記憶素子をリセットする手段 (12) を含むことを特徴とする回路。

## 【発明の詳細な説明】

## 【0001】

【発明の属する技術分野】 本発明は、集積回路からくるか又はそのような回路を含む電子サブアセンブリ素子からくる秘密量の使用に関する。例えば、本発明は、集積回路の識別又は認証のプロセスの秘密量として暗号鍵のようなプログラムによる、このような秘密量の使用に関する。より具体的には、本発明は、集積回路チップの製造に関連する、物理パラメータネットワークからくる集積回路のデジタル識別子の使用に関する。

## 【0002】

【従来の技術】 例えば集積回路チップを認証又はそれによって提供されるデータを符号化するための物理パラメータネットワークからくる識別子の使用は、集積回路中に隠された、又は埋め込まれた 2 進ワードを、不正コピーされる可能性のある記憶素子に一時的に記憶させずに使用することを可能にするため更に重要視されてきている。よって、起こり得る不正に対するシステムの信頼性は向上される。更に、物理パラメータネットワークの使用は所与の製造からくる異なる集積回路チップのための、互いに異なるデジタル識別子を得ることを可能にする。

【0003】 一般的には、集積回路のデジタル識別子は、遠隔システムに伝送するために可能な符号化又はスクランブルされた後、回路の外に提供される。後者 (スクランブル) は、受信したワードを使用し、識別子を知ることを必要としない。

【0004】 本発明の応用例は、プリペイド又はプリペイドでない会計ユニット (count unit) からの金融取引に用いられるスマートカード分野に関するものであり、その通信にはスマートカードリーダと接触するものではないものがある。

【0005】 もう 1 つの応用例は、ユーザ側に個人に特定されたデコーダを使用したデータ伝送システムである。そのような場合、デコーダは、そこに含まれる集積回路の物理パラメータネットワークからくる識別子を利用した認証回路を含んでもよい。支払システムにおけるスマートカードの例えで説明すると、認証がリーダとは異なるシステムによって行われる点を変えずに、リーダとそのスマートカードをユーザレベルで結びつけるのと同じことである。

【0006】 物理パラメータネットワークからくる識別子を使用することの不利は、その個別で固定的な性質と関連する。

【0007】 よって、侵害者が識別子又はこの識別子を含むデジタルワード (認証量又は符号化鍵) に対する海賊行為に成功すると、集積回路を換える以外に解決方法

はない。実際、識別子に海賊行為がなされたことが疑われたら即その識別子の使用を中止することが安全な応用においては望ましい。この現象は一般的に符号化鍵もしくは認証又はより一般的に秘密量の破棄、として知られている。

【0008】集積回路の物理パラメータネットワークの使用に基づいた鍵又は秘密量の破棄に対する解決策の欠如は、現在他の多くの用途に有利であるそれら識別子の使用を制限している。

【0009】

【発明が解決しようとする課題】本発明の目的は、集積回路における物理パラメータネットワークからくるデジタル識別子の既知の問題点を克服することである。

【0010】より具体的には、本発明の目的は、物理パラメータネットワークからくる識別子に基づいた秘密量又は鍵を、関わりのある集積回路を換えることなく破棄することを可能にすることである。

【0011】破棄する場合は、物理パラメータネットワークの数を増やすことによって、使用可能なデジタル識別子の数を増やしてもよい。しかしそのような解決策は、集積回路が大きくなってしまいう問題点がある。しかも使用できる識別子の数は、依然としてとても少ない。

【0012】更に、物理パラメータネットワークからくるワードのサイズより大きい秘密量のサイズは、検索されてしまう恐れがある。

【0013】本発明のもう1つの目的は、物理パラメータネットワークによって集積回路識別子の個々の特性を排除することのない解決策を提供することである。

【0014】また本発明は、集積回路の小型化と互換性のある解決策を提供することを目的とする。

【0015】また本発明は、秘密量を更に安全なものにするために、秘密量利用システム側にとって透過的である、つまり後者（利用する側）が使用される手段を知る必要のない解決策を提供することを目的とする。

【0016】

【課題を解決するための手段】これら及びその他の目的を達成するために、本発明は物理パラメータネットワークから最初のデジタルワードを発生させるステップと、前記最初のワードを少なくとも1つの遡及シフトレジスタに提示するステップとを含み、前記シフトレジスタの出力が前記秘密量を形成することを特徴とする、集積回路の識別子に基づく秘密量を発生する方法を提供する。

【0017】本発明の実施形態によると、前記最初のワードは、複数の遡及シフトレジスタに提示され、それらレジスタのうち1つが秘密量を形成するために選択される。

【0018】本発明の実施形態によると、前記選択は、先行の秘密量が破棄された後変更されるものとする。

【0019】本発明の実施形態によると、前記1つ又は

複数のシフトレジスタは線形遡及シフトレジスタである。

【0020】本発明の実施形態によると、シフトレジスタはセレクトタによって複数ある中から選択される。

【0021】本発明はまた、物理パラメータネットワークに基づく集積回路チップに特定な最初のデジタルワードの発生器と、前記最初のワードを入力として受け取り、前記量を提供する少なくとも1つの遡及シフトレジスタと、カウンタによってプログラム可能な前記シフトレジスタの導出シーケンス (derivation sequence) のセレクトタとを含むことを特徴とする、集積回路の内部で秘密量を発生する回路を提供することを目的とする。

【0022】本発明は更に、物理パラメータネットワークに基づく、集積回路チップに特定な最初のデジタルワードの発生器と、前記最初の2進ワードを入力として受け入れるものとする、いくつかの遡及シフトレジスタと、前記秘密量を提供する複数の前記遡及シフトレジスタのうち1つを選択するセレクトタとを含むことを特徴とする、集積回路の内部で秘密量を発生する回路を提供することを目的とする。

【0023】本発明の実施形態によると、前記セレクトタによって行われる選択は、秘密データを破棄する場合に変更されるものとする。

【0024】本発明の実施形態によると、セレクトタは、シフトレジスタの入力／出力から入力又は出力を選択するマルチプレクサにより形成されている。

【0025】本発明の実施形態によると、前記最初のワードと前記秘密量を記憶するレジスタは、一時的なレジスタであり、前記回路は、予め決められた時間の後でそれらの一時記憶素子をリセットする手段を含んでいる。

【0026】本発明の前述した目的、特徴及び効果は、添付図面に関連して、以下に限定しない特定の実施形態の説明において詳述される。

【0027】

【発明の実施の形態】明確にするために、集積回路の要素で本発明の理解に必要なもののみが図示され、以後説明される。具体的には、集積回路又は電子サブアセンブリ素子の構成部分であり本発明の物理パラメータネットワーク特性によって秘密量を発生することに関与しない部分については、示されていない。更に、本発明は、あらゆる従来の方に応用することができるため、秘密量の利用（例えば認証又は符号化のプロセスによる）については、集積回路の内外に関わらず詳述していない。

【0028】本発明の特徴は、少なくとも1つのシフトレジスタを、集積回路の製造に関連した最初のデジタルワードを提供する物理パラメータネットワーク、好ましくは線形遡及と結びつけることと、前記シフトレジスタによって提供されたデジタルワードを使用して集積回路の秘密量を形成することである。

【0029】本発明によると、複数の線形遡及シフトレ

ジスタが機能的に使用されている。レジスタの数は、集積回路の発生の中で物理的に増やされてもよく、又は単一シフトレジスタが提供され、以後述べられるように異なるビットの導出が提供されてもよい。

【0030】図1は、集積回路2の秘密量(KEY)を発生するためのセル1の実施形態を簡潔にブロックで表している。

【0031】セル1は、集積回路チップの製造に関わる物理パラメータネットワーク3(PPN)を含む。物理パラメータネットワーク3は、多数の信号を提供し、また、前記物理パラメータネットワークを表して一時的に記憶要素5(REG1)に記憶され、2進ワードを抽出する回路4と連結している。

【0032】例えば電気測定パラメータを含むあらゆるパラメータを使用することができる。それは例えばトランジスタのスレショルド電圧の測定、抵抗の測定又は浮遊容量の測定、電流源により発生された電流の測定、時定数(例えば、集積回路)の測定、振動周波数の測定等でもよい。それらの特性は、集積回路の技術的及び製造過程でのばらつきに影響されやすいため、考慮される電気パラメータはその製造に特定であり、その集積回路の署名を形成すると考えられる。

【0033】電気パラメータ測定の例において、信号は、アナログ-デジタル変換器によってデジタル信号に変換されてもよく、前記変換器は、抽出回路4を含み多重化されてレジスタ5に記憶される2進ワードを形成してもよい。

【0034】時間測定を使用した回路も、物理パラメータネットワークとして使用されることができる。例えば、EEPROM型メモリの読み出し/書き込み時間が測定される。この種類の物理パラメータネットワークの例は米国特許第5,818,728号において示されており、本発明の参考とした。

【0035】本発明の参考とした仏国特許出願第0104585号において示されているような、フリップフロップに基づいた物理パラメータネットワークも更に使用することができる。

【0036】本発明によると、鍵KEYは、物理パラメータネットワークから抽出した2進ワードを線形シフトレジスタに提示することにより得られる。

【0037】図1に示される実施形態では、n個の線形シフトレジスタ6(LFSR1、LFSRi、・・・、LFSRn)が提示されている。異なるレジスタのそれぞれは、例えばセレクタ7(SEL)に送られ、その出力が一時記憶要素8(REG2)において前記秘密量を提供する。あるいは、セレクタ7がレジスタ6の下流ではなく上流に配置されてもよい。

【0038】使用される線形レジスタの選択、つまりセレクタ7の制御は、カウンタ9(COUNT)によって発生させられた2進パラメータ化ワードに基づいて行わ

れ、よって前記カウンタは、現在の秘密量、即ち破棄されるまで使用される量を条件づける。セレクタはマルチプレクサでも、他の任意の従来の手段でもよい。

【0039】前記カウンタは、前回使用されたデータの破棄後、秘密データが変えられる度に歩進される。カウンタ9はシフトレジスタのモジュロ数値nである。

【0040】セル1は、集積回路1の安全な部分にあることが望ましい。「安全な部分」とは、直接電気測定による攻撃から保護されている部分である。例えばそれは、侵害者がその内容を検出しようとした場合溶解温度によってセルが破棄されるように、樹脂に埋め込まれたセルでもよい。

【0041】図示されていないもう1つの実施形態によると、導出されたビットがパラメータ化される単一の線形シフトレジスタが使用される。この特徴は、以後図2及び図3との関連によって更に明らかになる。

【0042】発生セル1は更に、それを形成する異なる要素を制御するためのセントラルユニット12(CU)を含む。セントラルユニット12は、秘密量の発生の制御信号を必要とときに、好ましくは一時的な方法で受けるため、また、破棄後の新しい秘密量の発生に必要な制御信号、つまりカウンタ9の増加(又は減少)を誘発する制御信号を受けるため、他の部分と共に集積回路の残りの部分と通信する。

【0043】秘密量を使用するシステムは、秘密量KEYを処理するだけであってそれを発生させる方法を知る必要はない、という点が注目される。よって、本発明による発生セルは、秘密量の利用に対して透過的であり、よってあらゆる従来の利用法と互換性がある。

【0044】他の方法としては、カウンタ9がセレクタ7を形成する多重化装置の選択コードのリストと置き換えられる。それらコードは使用に先立ってパラメータ化段階で揮発性メモリに記憶される。

【0045】線形シフトレジスタの使用は、秘密量の破棄を可能にすること、実現が容易であること、又より具体的に、先行の量を破棄する際集積回路の秘密量の変更を可能にする点で好ましく、一方、物理パラメータネットワークからくる識別子を利用し、そして特にそのような識別子は電気測定によって侵害できない、という利点を有する。

【0046】図2は、遡及シフトレジスタの全体的な構成図である。このようなレジスタは、基本的にシフトレジスタ20と遡及機能21(RETROACT)の2つの部分から成る。シフトレジスタ20は任意のシフトレジスタ同様ビットB1、B2、B3、・・・、Bm-1、Bmの連続を形成する。遡及機能を形成するブロック21の機能は、ビットの連続のシフト毎に、レジスタに含まれるビットの少なくとも一部分の組み合わせに基づいて、シフトレジスタ(ビットBm)の入力ビットを計算することである。よって、シフトレジスタ20の各

ビットを遡及機能21に個別に提供することができる。シフトレジスタ20の出力は、直列形で該レジスタの2進ワードの最下位のビットB1によって形成される。並列出力の実施形態では、検索されたワードによって、前記シフトレジスタの全てのビットの値又はこれらビットの一部が同時にサンプリングされる。

【0047】シフトレジスタの使用は、その実現がとりわけ容易である点で好ましい。遡及機能としては、任意の従来の機能が使用されることが可能である。出力として再生可能なワードを発生することが可能であるならば、非線形遡及機能の使用が考慮されてもよい。しかし、本発明の実施形態によると、前記シフトレジスタのいくつかのビットをXOR型に組み合わせた線形遡及機能が使用されている。これらビットのリストは一般的に「導出シーケンス (deriving sequence)」、又は「フィボナッチ構成 (Fibonacci configuration)」という表現によって示されている。

【0048】シフトレジスタに含まれる2進ワードの反復期間は、このレジスタのビット数だけではなく使用される遡及機能による。mビットの線形シフトレジスタにおいては、 $2^m - 1$ の異なる2進シーケンスを使用できる。つまり、適応サイズのレジスタの出力OUT上に提供される連続したビットをロードすることにより、 $2^m - 1$ ビットまでの間のサイズの秘密量を得ることができる。これは、反復前で最も長いワードを形成する。線形シフトレジスタによって提供されたコードのアンローディングの連続を使用する事実は、物理パラメータネットワークによって提供されたワードの長さについて、秘密量を長くすることを可能にする。

【0049】動作を分かりやすくするために、図3は導出シーケンスがB1、B4である4ビットの線形シフトレジスタを簡潔に表したものである。つまり、レジスタ20'に含まれ、4ビットを超えるそれぞれ最下位のビットと最上位のビットであるB1及びB4は、遡及機能を形成するXOR型ゲート21'によって結合される。ゲート21'の出力はシフトレジスタ入力を形成し、よってB4入力となる。出力シーケンスOUTは最下位ビット(B1)によって提供される。

【0050】値を1000として初期化すると仮定すると、つまり、他のビットを全て0にリセットした後B4に状態1をロードすると、レジスタ20'の連続した内容は反復前に1000; 1100; 1110; 1111; 0111; 1011; 0101; 1010; 1101; 0110; 0011; 1001; 0100; 0010; 0001となる。

【0051】本発明によれば、可能な組み合わせの数による反復前の導出周波数の選択は、当業者であれば行うことができる。線形シフトレジスタの実現は、ハードウェア又はソフトウェアどちらの形であっても、全く従来どおりである。例えば、本発明の参考としたBruce Schnei

er著、Wileyにより出版された、第395～第401頁、「応用暗号法」第2版、を参照することができる。

【0052】ネットワーク3からきて、レジスタ6の初期シーケンスの設定に使用されるワードは、直列又は並列でロードすることができる。レジスタ6の初期値を設定することにより、ユニット12に制御されかつ好ましく予め決められた条件であるシフトレジスタの数は、再生可能な方法で得られた最終ワードを提供する。

【0053】導出シーケンスを変更(図1のnの連続のレジスタ6をもう1つ選択するのと同じことである)することによって、同一の入力ワード(mより大きい同じ数のシフトサイクルを持つ)のために得られた前記ワードが変更される。他の方法として、秘密量を変更するためにシフトサイクルの数を変更されてもよい。

【0054】

【発明の効果】本発明の利点は、破棄防止方法 (anti-evocation procedure) の要素をデータ利用システムに提供せずに、物理パラメータネットワークからくる2進ワードから得られた秘密量の破棄に関する問題を解決できる点である。よって、本発明により提供された解決策はとりわけ信頼性があり安全である。

【0055】本発明の利点はいくつかの鍵の破棄を承認しながら1つの物理パラメータネットワークを使用できるという点である。

【0056】本発明のもう1つの利点は、物理パラメータネットワークからくるワードの抽出に基づく秘密量の揮発性の(一時的)特性を保持できるという点である。

【0057】もちろん、本発明は当業者であれば様々な改変、変更、改善等が容易に思いつくだらう。具体的には、使用される2進ワードの長さは応用によるものであり、本質的には集積回路に使用される認証プロセスによるものである。この点において、本発明は集積回路に提供された秘密量の既存の利用方法と互換性があると言える。

【0058】更に、以上述べた機能的指示に従った遡及シフトレジスタの実施の実現は、線形であるか否かによらず当業者であれば行うことができる。シフトレジスタを複数使用するかレジスタを1つ使用するかの選択と、スイッチにより選択される導出シーケンスは例えば記憶素子とシフトレジスタの間で何が優先されるのが望ましいかによって行われることができる。

【0059】更に、シフトサイクルの数は、所与の鍵に対して同じであれば重要ではない。破棄に伴う鍵の変更の際には他のサイクル数の設定も可能であり、それが同じ導出シーケンスを継続してもしなくてもよい。

【0060】最後に、本発明はこれまでハードウェアの実現との関連をより詳しく説明してきたが、ソフトウェアの手段としても実現されることができる。

【0061】このような変更、修正及び改良は、この開示の部分でしようとするものであり、本発明の思想及び

範囲の中で行われるものである。従って、前述した記載は、単に例としてであり、限定しようとするものではない。本発明は、特許請求の範囲及びその均等範囲によって規定するもののみに限定される。

#### 【図面の簡単な説明】

【図1】本発明による秘密量を発生するための回路の実施形態をブロックで表した概要図である。

【図2】図1の回路で使用される線形逡及シフトレジスタのブロック図である。

【図3】第1及び第4ビットが導出された4ビットの線形逡及シフトレジスタの簡単な例である。

#### 【符号の説明】

1 セル

2 集積回路

3 物理パラメータネットワーク

4 発生器、抽出回路

5 レジスタ、記憶素子

6 逡及シフトレジスタ、線形シフトレジスタ

7 セレクタ

8 レジスタ、一時記憶素子

9 カウンタ

12 セントラルユニット

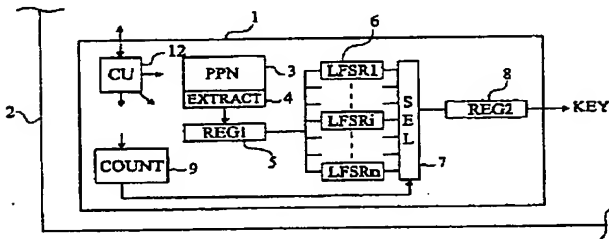
20 シフトレジスタ

20' レジスタ

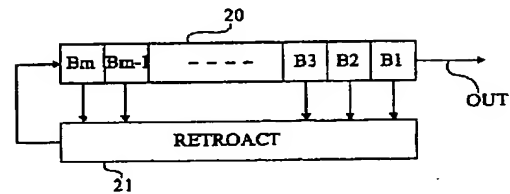
21 逡及機能

21' ゲート

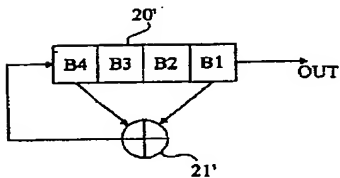
【図1】



【図2】



【図3】



フロントページの続き

(72)発明者 ミシエル バルドウイエ  
フランス国、13790 ルーセット、カ  
ルティエ フォンジュアーヌ

(72)発明者 ローラン プラザ  
フランス国、13710 フェヴォー、リ  
ュドゥ ジュー デ ブーレ、レジダ  
ンス レ クロ

Fターム(参考) 5B035 AA13 BB09 CA11  
5J104 AA16 AA18 EA08 FA04 NA04  
NA22 NA23 NA25 NA26